STATE OF ALABAMA

Information Technology Standard

Standard 640-03S2: Wireless Clients

1. INTRODUCTION:

WLAN-capable devices typically are at greater risk of a security breach than wired-only devices and may require additional security controls beyond those already present. This standard describes how wireless client devices are to be deployed, managed and utilized by State of Alabama organizations. It covers wireless-capable laptop PCs, personal digital assistants (PDA), text-messaging devices and smart phone-PDA products.

2. OBJECTIVE:

Ensure all organizations deploy, manage, and/or utilize wireless technologies with an acceptable level of security.

3. SCOPE:

These requirements apply to wireless client devices used to connect to the State of Alabama network.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-48: Wireless Network Security, and NIST Special Publication 800-97: Guide To IEEE 802.11i: Establishing Robust Security Networks, State of Alabama organizations that deploy, manage, or utilize wireless networks shall comply with the following requirements.

Only FIPS validated 802.11i solutions using IEEE 802.1X/EAP authentication (rather than pre-shared keys) are approved for use on State networks. Legacy wireless clients that do not support 802.11i and WPA-2 shall utilize a State-approved Virtual Private Network (VPN) solution configured in accordance with applicable State standards.

Establish or enhance operating system and application security configuration standards for laptops and other wireless devices to account for WLAN risks.

Install state-approved personal firewall and anti-virus software for all wireless devices for which such security products are commercially available.

Ensure that the client devices connecting directly to the State network connect only to a valid authentication server (AS). To ensure authorized connections, the device should be configured to specify the names of valid ASs, specify the locally stored certification authority (CA) certificate used to validate the digital signature of the AS certificate, and require that the device check for AS certificate revocation.

Disable ad hoc mode on wireless devices.

Wireless devices shall undergo security assessments to identify security vulnerabilities.

Ensure wireless devices are stored securely when left unattended.

When practical use physical locks and cables to minimize the risk of loss or theft.

Synchronize devices with their corresponding PCs regularly to ensure data availability.

Ensure desktop application mirroring software is password protected.

Turn off communication ports during periods of inactivity, when possible, to minimize the risk of malicious access.

Wireless access and authentication shall comply with normal network access policies and procedures (i.e., password standards, log-in attempts, lock-out policy, etc).

Ensure all devices utilize timeout mechanisms that automatically prompt the user for a password after a 30-minute period of inactivity.

When disposing of a wireless device, remove all sensitive data and configuration information using one (or more) of the following methods:

- Use degauss devices when feasible,
- Disk wiping utilities can be used for devices that have hard disks, or
- Clear configuration settings manually using the management interface.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-03: Wireless Security

6.2 RELATED DOCUMENTS

Information Technology Standard 640-03S1: Wireless Networks

Information Technology Standard 640-03S3: Bluetooth Security

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	2/16/2007	